Department of Homeland Security IAIP Directorate Daily Open Source Infrastructure Report for 22 June 2005

Current Nationwide Threat Level is

ELEVATED
SIGNIFICANT RISK OF TERRORIST ATTACKS

For info click here
http://www.dhs.gov/

Daily Highlights

- The Associated Press reports the criminal exploit that exposed 40 million credit card accounts to possible fraud shows a critical area of the financial industry: the hundreds of companies that process transactions between merchants and card issuers. (See item 5)

- San Antonio Express News reports the Arizona Minuteman group has established its first Texas affiliate in Goliad, in response to local frustration over the ongoing flow of illegal immigration. (See item 13)

- The Department of Homeland Security and other federal departments and agencies are testing their continuity of operations plans this week during Exercise PINNACLE, an effort to improve the ability of government to perform essential functions during threats and emergencies. (See item 21)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: Elevated, Cyber: Elevated
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://esisac.com]

1. *June 21, Detroit News* — **Michigan may face power crisis.** Michigan could face an electric power crisis in the near future −− with the threat of brownouts and even blackouts −− because uncertainties about electric competition make the climate too unstable to entice anyone to build a power plant, say officials across the electric industry. The state's power grid is expected to

hold up this summer, as evidenced by lack of troubles through the season's heat wave earlier this month. However, experts wonder how many more peak demand seasons the state can endure. In a state where utilities are half in and half out of a regulated market and electric choice for customers struggles to take hold, the prospect for a new plant any time soon appears dim. "Unless there is a stable regulatory environment, nobody −− no marketer, no independent power producer, no regulated utility −− will build another base load plant in Michigan," said DTE Energy Chief Anthony Earley Jr. "Right now there is enough generation to supply us, but two or three years down the road you're going to start having some real reliability problems," said Earley. Meanwhile, demand for electricity is growing 1.5 to three percent a year.
Source: http://www.detnews.com/2005/business/0506/21/A01−222595.htm

2. *June 21, Associated Press* — **Oil peak not coming soon according to report.** Global oil production is not likely to peak anytime soon, contrary to talk that has helped propel prices to $60 a barrel, a prominent energy consultancy said Tuesday, June 21. Cambridge Energy Research Associates (CERA) said that, instead of a crest being reached sometime this decade, an inflection point in world oil output will occur sometime beyond 2020, after which production will plateau for several more decades. In a report that builds upon earlier analyses by the Cambridge, MA−based consultancy, CERA said it believes that between now and 2010 there will be a substantial increase in worldwide oil production capacity. It said that "as a result, supply could exceed demand by as much as six million to 7.5 million barrels per day later in the decade" that will lead to an extended period of lower prices beginning as early as 2008. "Today's high prices are the result of an exceedingly tight and precarious supply−demand balance," CERA chairman Daniel Yergin said in a statement. "Yet significant new capacity will be coming on stream....The addition of that new capacity is what is required to improve the supply demand balance."
CERA: http://www.cera.com/news/details/1,2318,7453,00.html
Source: http://www.nytimes.com/aponline/business/AP−Oil−No−Peak−Yet. html?

3. *June 20, Nuclear Regulatory Commission* — **Nuclear Regulatory Commission completes restoration of documents.** The Nuclear Regulatory Commission (NRC) on Friday, June 17, completed the restoration of public access to an additional 70,000 documents through its online library, ADAMS, after conducting a security−sensitivity review. Members of the public are now able to access these documents, involving administrative, contractual, research and other documents not related to a specific licensee, which were removed from the public library on October 25 of last year. “We are pleased that the public will once again be able to obtain these documents,” said Edward T. Baker, Director of the NRC’s Office of Information Services. “While we are firmly supportive of openness in our regulatory process, it was important to remove these documents to conduct a security review and remove information that could potentially be of use to a terrorist,” said Baker. The agency has previously restored access to about 163,000 non−sensitive documents. It continues to evaluate documents dealing with nuclear materials licensees.
Source: http://www.nrc.gov/reading−rm/doc−collections/news/2005/05−0 94.html

[Return to top]

Chemical Industry and Hazardous Materials Sector

4. *June 21, The Baytown Sun (TX)* — **Chemical exposure led to contractor’s death.** KBR employee Salvador Barba died after being exposed to the chemical phenol following an accidental release Saturday morning, June 18, at the Bayer Industrial Park, in Baytown, TX. “There was no fire or explosion. No one else was injured. The incident at no time posed a threat to the community,” said Bayer Baytown spokesperson Cherie Laughlin. Plant manager John Rocco said that Bayer and KBR employees immediately rushed to Barba’s aid, and the plant’s emergency team responded within a minute of the exposure. According to the federal Agency for Toxic Substances and Disease Registry, phenol, more commonly called carbolic acid, is a colorless−to−white manufactured substance used in a variety of industrial processes. According to the National Safety Council, very high concentrations of phenol can cause death if ingested, inhaled or absorbed through the skin. Laughlin said that Bayer and KBR safety management officials have begun an investigation of the cause of the chemical release, while Rocco stated that the polycarbonate facility has been shut down and barricaded until the Occupational Safety and Health Administration (OSHA) officials give approval.
Source: http://www.baytownsun.com/story.lasso?wcd=21774

[Return to top]

Defense Industrial Base Sector

Nothing to report.
[Return to top]

Banking and Finance Sector

5. *June 21, Associated Press* — **Security leak reveals weaknesses in credit card processing system.** The criminal exploit that exposed 40 million credit card accounts to possible fraud is shedding light on an arcane but sensitive piece of the financial industry: the hundreds of companies that process transactions between merchants and card issuers. While enormous in scope, the breach disclosed Friday, June 17, at CardSystems Solutions Inc. was by no means the first such attack on a card processor. Many analysts believe that banks and credit card companies, despite working hard to tighten their own security, have failed to force payment processors to maintain similar standards. "They're not being watched carefully enough," said Avivah Litan, an analyst with Gartner Inc. In recent years, card associations such as Visa and MasterCard have set up security requirements for processors to follow. No laws in particular govern this program, but the card associations can impose fines of several hundred thousand dollars for transgressions. However, Litan said proactive audits of companies like CardSystems don't really happen. Credit card companies "just sort of wait for them to have a breach," she said. "There's just a lot of vagaries in how it's enforced," said Litan.
Source: http://www.informationweek.com/showArticle.jhtml;jsessionid=ALTUJC33UI0AGQSNDBCCKH0CJUMEKJVN?articleID=164901395

6. *June 21, New York Times* — **Black market in stolen credit card data thrives on Internet.** Despite years of security improvements and tougher, more coordinated law enforcement efforts, the information that criminals siphon −− credit card and bank account numbers, and whole buckets of raw consumer information −− is boldly hawked on the Internet. The data's value

arises from its ready conversion into online purchases, counterfeit card manufacture, or more elaborate identity theft schemes. The online trade in credit card and bank account numbers, as well as other raw consumer information, is highly structured. There are buyers and sellers, intermediaries and even service industries. The players come from all over the world, but most of the Websites where they meet are run from computer servers in the former Soviet Union, making them difficult to police. Traders quickly earn titles, ratings and reputations for the quality of the goods they deliver. Also, a wealth of institutional knowledge and shared wisdom is doled out to newcomers seeking entry into the market, like how to move payments and the best time of month to crack an account. No one is willing to estimate how many cards and account numbers actually make it to the Internet auction block, but law enforcement agents consistently describe the market as huge.
Source: http://www.nytimes.com/2005/06/21/technology/21data.html

7. *June 20, TechWeb News* — **Phishers take advantage of MasterCard breach.** When MasterCard went public last week with news that a security breach exposed more than 40 million cards to fraud, customers weren't the only ones interested. Phishers picked up on it, too, and quickly launched a campaign to piggyback on the blunder. The e−mail reads in part: "During our regular update and verification of the accounts, we couldn't verify your current information." Although it makes no specific reference to the security breach −− likely because the message and bogus Website were already taken down −− the campaign could have more legs than usual, because card customers who read the news will be expecting to hear from MasterCard or their issuing bank about how the security problem affects them.
Source: http://www.techweb.com/wire/security/164901129

8. *June 20, Reuters* — **Hackers score big by thinking small.** A recent computer security breach that left 40 million credit cards vulnerable to fraud shows how online criminals are scoring big by thinking small, experts said on Monday, June 20. Cybercriminals are increasingly crafting more focused attacks with a potential for profit as they target one or two companies at a time, rather than blasting out Internet virus attacks across the globe, according to security experts. "We have seen several examples of targeted, manually crafted Trojans that people write and implement for a very small number of companies," said Aladdin Security Vice President Shimon Gruper. MessageLabs chief technical officer Mark Sunner said that since January the company has seen a 150 percent increase in attacks that only target one or two companies. A key advantage of targeted attacks is that they are usually small enough to stay off the radar of Internet security firms that are looking for broader attacks. That gives the high−tech criminals the time to research a company thoroughly before trying to penetrate it.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2005/06/20/AR2005062000906.html

9. *June 20, IDG News Service* — **Banks to spend more on IT security, survey says.** Investment in security has topped the banking sector's IT spending priority list for 2005, according to a study by the Info−Tech Research Group. Info−Tech's 2005 IT Budget and Staffing Report surveyed more than 1,400 IT decision−makers in various vertical industries, including finance, manufacturing, government, agriculture, health and professional services. Of the banks surveyed, 89% were in based in the U.S. Privacy regulations and other compliance challenges are the main factors driving banks to spend more to improve their security infrastructure, according to Jason Livingstone, an analyst at London, Ontario−based Info−Tech. Of the banks

surveyed, 59% said they're planning to increase their investment levels for security, focusing on privacy and security of transactions. Seventy percent of the banks' IT executives said they will spend money on security software. Banks are ahead of companies in other sectors when it comes to implementing security technologies such as firewalls, virtual private networks, and antispam and intrusion−detection systems, with 80% saying they have adopted at least one of those systems, the survey said.
Report information: http://www.infotech.com/Products%20and%20Services/IT%20Budget%20and%20Staffing/Banks.aspx
Source: http://www.computerworld.com/managementtopics/management/itspending/story/0,10801,102642,00.html

[Return to top]

Transportation and Border Security Sector

10. *June 21, Associated Press* — **Chicago says it doesn't have money for key component of airport expansion project.** The planned expansion of Chicago's O'Hare International Airport is in difficulty since the city says it doesn't have money for a $250 million taxiway and the federal government insisted the aircraft access road be built. The Federal Aviation Administration (FAA) told city aviation officials last week that they must guarantee that the "LL" taxiway will be built by the time Runway 10 Center/28 center is opened. The taxiway is a critical element in the city's $6.6 billion airport expansion project designed to dramatically reduce delays at O'Hare and increase the airport's capacity to handle hundreds of thousands of additional flights a year. "We don't want to get into the situation of bringing planes across the middle of an active runway," FAA spokesperson Tony Molinaro said. "That would require adding space between flights and slowing down everything to ensure safety." Runway incursions −− two aircraft in the same space at the same time −− are the top cause for commercial accidents. Though most incursions are caused by pilot or controller errors, airfield design has been a factor in some collisions. The FAA encourages airports to be designed so that planes taxi around runways whenever possible because such designs limit runway incursions.
Source: http://www.usatoday.com/travel/flights/2005−06−20−ohare−expa nsion_x.htm

11. *June 21, Associated Press* — **Fourth big airport may be needed in metro NYC.** Chairman Anthony Coscia, head of the Port Authority of New York and New Jersey, said Monday, June 20, that the metropolitan region may need a fourth major airport to meet the great demand for air travel. Coscia also said his agency has asked federal regulators to reduce flights in and out of Teterboro Airport, where two planes have skidded off runways and a third crashed while landing this year. Located in a densely populated area near New York, Teterboro has grown into one of the nation's busiest small airports. Closing the airport, they said, is not an option because it employs 1,200 people and contributes $1.8 billion to the economy each year. LaGuardia, Newark Liberty and John F. Kennedy international airports all serve the area. Coscia said adding an airport to the region, to which about 100 million people travel for business and pleasure annually, is worth considering. "Whether that includes a fourth major airport, whether that includes additional capacity, all of those things should be on the table and we're going to spend the resources on studying it intelligently because what we don't want to do is to see the problems that we have today at Teterboro," Coscia said.
Source: http://www.usatoday.com/travel/flights/2005−06−20−nyc−airpor ts_x.htm

12. *June 21, Government Technology* — **Connecticut E−Alert traffic system has 4,091 subscribers in first three months.** Connecticut Governor M. Jodi Rell announced that 4,091 people have signed up for the Department of Transportation's statewide electronic rail and highway traffic incident notification system in just its first three months of operation. "Improving our transportation system is my top priority, and I will continue to press for positive change whenever and wherever possible," Governor Rell said. "The feedback from commuters about our e−alert system has been overwhelmingly positive. The system has been working well and the information it provides is very useful." The service is available −− at no cost −− 24 hours a day, seven days a week to subscribers with access to electronic mail. Notice of significant highway incidents expected to last at least an hour are e−mailed to subscribers. Incident updates and notification when an incident has been cleared are also provided.
E−Alert Website: http://www.ct.gov/dot/cwp/view.asp?a=2003&Q=290292&dotNav=|
Source: http://www.govtech.net/news/news.php?id=94354

13. *June 21, San Antonio Express News (TX)* — **Minutemen start Texas branch.** The Arizona Minuteman Project established its first Texas affiliate in Goliad Monday, June 20, responding to local ranchers frustrated with the government's inability to stem the flow of illegal immigration. More than 200 people attended the organizational meeting at Goliad Memorial Auditorium. The Arizona Minuteman Project drew international attention in April when it enlisted volunteers from across the country to help patrol a 23−mile stretch of the Arizona border. The group claims its efforts reduced illegal immigration there with little violence and has set out to extend their project to New Mexico, Texas and California. Chris Simcox, a chief organizer for the Arizona Minuteman Project and founder of the Minuteman Civil Defense Corps, told the audience that he has received enough interest in Texas to form four chapters of the Minuteman Project in cities such as Odessa, Midland and Houston. He said the group wouldn't stop until its goal is of bringing military troops to patrol the border is met. About 50 area ranchers called Simcox and his group after noticing a surge of illegal immigrant activity in Goliad County in the past year.
Source: http://www.mysanantonio.com/news/metro/stories/MYSA2005621..
NZ.Metro.minutemen_metro_0621.2f6a8aa5.html

14. *June 21, Government Accountability Office* — **GAO−05−651T: Coast Guard: Preliminary Observations on the Condition of Deepwater Legacy Assets and Acquisition Management Challenges (Testimony).** In 2002, the Coast Guard began a multiyear, $19 billion to $24 billion acquisition program to replace or modernize its fleet of deepwater aircraft and cutters, so called because they are capable of operating many miles off the coast. For several years now, the Coast Guard has been warning that the existing fleet −− especially cutters −− was failing at an unsustainable rate, and it began studying options for replacing or modernizing the fleet more rapidly. Faster replacement is designed to avoid some of the costs that might be involved in keeping aging assets running for longer periods. This testimony, which is based both on current and past Government Accountability Office work, addresses several issues related to these considerations: (1) changes in the condition of deepwater legacy assets during fiscal years 2000 through 2004; (2) actions the Coast Guard has taken to maintain and upgrade deepwater legacy assets; and (3) management challenges the Coast Guard faces in acquiring new assets, especially if a more aggressive schedule is adopted.
Highlights: http://www.gao.gov/highlights/d05651thigh.pdf

Source: http://www.gao.gov/cgi−bin/getrpt?GAO−05−651T

[Return to top]

Postal and Shipping Sector

Nothing to report.
[Return to top]

Agriculture Sector

15. *June 21, Organization for Economic Co−operation and Development* — **Agriculture export competition to intensify.** Global competition among exporters of wheat, rice, oilseeds, sugar, and livestock is expected to intensify over the next ten years among both developed and developing countries, according to the Organization for Economic Co−operation and Development's (OECD) latest Agricultural Outlook −− produced for first time in collaboration with the United Nation's Food and Agriculture Organization (FAO). Stiffer competition, combined with higher productivity, will result in a further drop in real prices for most basic food commodities. Although increasing imports by China and other Asian countries could drive nominal prices higher in the near term, international wheat prices are expected to fall in real terms by around 11 percent over the next 10 years. With the growing importance of China and India in global markets, small shocks to either demand or supply in these large countries could lead to substantial external adjustments. Similarly, conditions in the key emerging suppliers, particularly in South America, will be increasingly critical to the evolution of world markets. With rapidly increasing production and trade of livestock products, animal disease outbreaks also provide for an important source of uncertainty.
Agricultural Outlook report:
http://www.oecd.org/document/5/0,2340,en_2649_201185_3501594_1_1_1_1_1,00.html
Source: http://www.oecd.org/document/8/0,2340,en_2649_201185_3501984
8_1_1_1_1,00.html

16. *June 20, Associated Press* — **Colorado city to track deer with chronic wasting disease.** Boulder, Colorado’s Open Space and Mountain Parks Department wants to study chronic wasting disease (CWD) in a radically new way, tracking infected deer instead of killing them. They are proposing capturing between 100 and 120 deer, testing them for the disease, tagging them with radio collars, then releasing them back into the wild to find out how the disease affects the animals that contract it and how it spreads. “It’ll be the first study of its type, probably, in the entire U.S., that attempts to look at the survivorship of infected animals and healthy animals,” said Charles Southwick, a University of Colorado ecologist who is serving as a consultant to the program. Wildlife managers have been dealing with CWD by killing deer in “hot spot” populations where the disease has been found, hoping to reduce its prevalence. Southwick and others say that approach is flawed because otherwise healthy deer are often killed.
Source: http://www.lovelandfyi.com/region−story.asp?ID=983

[Return to top]

Food Sector

Nothing to report.
[Return to top]

Water Sector

Nothing to report.
[Return to top]

Public Health Sector

17. *June 21, Agence France Presse* — **China reports new outbreak of bird flu.** China has reported a new outbreak of deadly bird flu as it denied encouraging farmers to use a drug meant for humans to treat infected poultry, a practice that could render the medicine useless. The outbreak, the third revealed by China in the past two months, occurred at a farm in northwest China's Xinjiang region. At least 128 geese and ducks were infected and 63 of them were killed by the H5N1 strain of the virus, the United Nation's Food and Agriculture Organization (FAO) said. Authorities have culled 1,490 birds in the infected farm and nearby areas in Changji city, said an FAO official. A ministry official, meanwhile, refuted a Washington Post report claiming Chinese farmers, with government backing, had widely used the human flu drug amantadine to combat the deadly virus in poultry since the 1990s. Experts warn that such misuse increases the resistance of the virus to the antiviral drug, with potentially deadly consequences if the bird flu bug should ever mutate to spread easily among humans.
Source: http://news.yahoo.com/s/afp/20050621/hl_afp/healthfluchina_0 50621114245

18. *June 21, Associated Press* — **Encephalitis found in mosquitoes in Nevada.** A second pool of mosquitoes in northern Nevada has tested positive for encephalitis, this time in Lyon County, state officials said. The Nevada Department of Agriculture notified the Mason Valley Mosquito Abatement District on Friday, June 17, that a pool of mosquitoes at a rest area near Wilson Canyon had tested positive for St. Louis encephalitis. The virus passed to humans by mosquitoes causes flu−like symptoms and in some cases death, though such incidents are rare, officials said. It's the second confirmation of mosquitoes having encephalitis in the state this year. The first was detected in Churchill County earlier this month.
Source: http://www.lasvegassun.com/sunbin/stories/nevada/2005/jun/21 /062110726.html

19. *May 31, Infectious Diseases Society of America* — **African HIV subtypes identified in Minnesota population.** Public health researchers in Minnesota recently identified 83 persons infected with subtypes of HIV−1 that are not common in the U.S. Viral subtype identification may be important because subtypes may differ in terms of the efficacy of potential vaccines, diagnostic testing for HIV infection, and monitoring of the health of HIV−infected patients. The report, by Tracy L. Sides, MPH, and colleagues of the Minnesota Department of Health and the HIV Program at Hennepin County Medical Center, emphasizes the need for better surveillance of HIV−1 subtypes to determine their prevalence. For the first two decades of the AIDS epidemic in the U.S., HIV−1 subtype B has been the predominant isolate throughout the

country. In recent years, non−B HIV−1 subtypes have been spreading in parts of Europe. As Sides and colleagues explained, however, the prevalence of subtype B and other subtypes in the U.S. is not known, because subtype testing is not conducted with routine HIV/AIDS surveillance. In 2003, the Minnesota Department of Health piloted HIV−1 subtyping with routine surveillance to describe and monitor non−B−subtype HIV−1 isolates.
Research: http://www.journals.uchicago.edu/JID/journal/issues/v192n1/3 3693/33693.html
Source: http://www.idsociety.org/Template.cfm?Section=News_from_the_ Journals&CONTENTID=12879&TEMPLATE=/ContentManagement/Content Display.cfm

[Return to top]

Government Sector

20. *June 21, Government Accountability Office* — **GAO−05−838T: Courthouse Construction: Overview of Previous and Ongoing Work, by Mark L. Goldstein, director, physical infrastructure (Testimony).** Over the last 20 years, the Government Accountability Office (GAO) has compiled a large body of work on courthouse construction and federal real property. The General Services Administration (GSA) owns federal courthouses and funds related expenses from its Federal Buildings Fund (FBF)–a revolving fund used to finance GSA real property services, including the construction and maintenance of federal facilities under GSA control. The judiciary pays rent to GSA for the use of these courthouses, and the proportion of the judiciary’s budget that goes to rent has increased as its space requirements have grown. In December 2004, the judiciary requested a $483 million permanent, annual exemption from rent payments to GSA to address budget shortfalls. In this testimony, GAO (1) summarizes its previous work on courthouse construction and (2) provides information on FBF and GAO’s ongoing work on the federal judiciary’s request for a permanent, annual rent exemption of $483 million from rent to GSA.
Highlights: http://www.gao.gov/highlights/d05838thigh.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−05−838T

[Return to top]

Emergency Services Sector

21. *June 20, Department of Homeland Security* — **DHS announces exercise to test continuity of operations plans.** As part of the ongoing efforts to test and improve the ability of government to perform essential functions during threats and emergencies, the Department of Homeland Security (DHS) and other federal departments and agencies are testing their continuity of operations (COOP) plans this week during Exercise PINNACLE. The exercise will allow federal officials to implement COOP plans, test communications connectivity, and demonstrate that essential functions can be effectively conducted during threats and emergencies. Similar to the “Forward Challenge” exercise conducted in May 2004, Exercise PINNACLE will also include a hypothetical terrorism scenario and accompanying emergencies that require COOP activities to be conducted by the Federal government. The Exercise scenario is not based on any specific threat or intelligence information. Unlike the recent “TOPOFF Exercise” which involved real life response capabilities using assets and personnel from Federal. state and local

governments, Exercise PINNACLE will simply test operations and procedures for performing essential government functions during threats and emergencies.
Source: http://www.dhs.gov/dhspublic/display?content=4547

22. *June 20, Daily Herald (IL)* — **Illinois police find use for Homeland Security grants.** Police and sheriff's departments across Illinois this year received 215 grants totaling nearly $6.78 million through the Illinois Terrorism Task Force, the state agency responsible for developing plans for responding to terrorist attacks. Todd Kupsak, grants coordinator for the Buffalo Grove Police Department, said this is the second straight year the village has received the grant. Last year, the department received $50,000, which it used for a portable surveillance system. It enables police to conduct surveillance from a squad car or a station house without putting officers in harm's way. Kupsak said the grant was written with the protection of critical infrastructure from terrorists in mind. Targets could include gas lines, water lines and the police campus itself. Of particular concern in Buffalo Grove was the protection of the community's many synagogues. The camera system purchased with last year's grant, a unit resembling an electrical box, could be installed anywhere and has the dual advantage of being inconspicuous and damage proof. Kupsak said this year's grant of $11,430 will update camera systems in the police department itself.
Source: http://www.dailyherald.com/news/cookstory.asp?id=63645

23. *June 20, Federal Emergency Management Agency* — **DHS Under Secretary calls on fire departments nationwide to make health and safety a priority.** Michael D. Brown, Under Secretary of Homeland Defense for Emergency Preparedness and Response and head of the Federal Emergency Management Agency (FEMA), called on America's firefighters to step aside from routine duties Tuesday, June 21, 2005, and "stand down" to focus on their own health and safety. FEMA, which includes the U.S. Fire Administration is joining 20 other organizations in the first−ever National Stand Down Day for Firefighter Health and Safety. Firefighter injury and death rates have remained relatively constant over the past several years, despite monumental improvements in technology and equipment. In a given year, about half the line−of−duty deaths are from heart−related illnesses. Another 25 percent are from accidents including motor−vehicle accidents. The initiative, led by the International Association of Fire Chiefs, calls for firefighters on all shifts over the next week to put aside routine duties like alarm inspections and building maintenance for one shift. All fire departments will still answer all emergency calls, but when there are no emergency calls, firefighters will concentrate their efforts on being healthier and safer on and off the job. The National Fire Protection Association cites more than 78,000 firefighter injuries annually.
Source: http://www.fema.gov/news/newsrelease.fema?id=17814

24. *June 20, The El Dorado Times (KS)* — **Kansas hospital holds decontamination team drill.** Patients began showing up at Susan B. Allen Memorial Hospital's emergency room in El Dorado, KS, on Tuesday, June 14, complaining of symptoms related to their exposure to some kind of chemical spill. It was subsequently determined those patients had been exposed to benzene. Gene Kimble, the hospital's director of marketing, said Tuesday's exercise was the first true complete drill the hospital's decontamination team has gone through in which simulated patients have been involved. Tuesday's drill was designed to help familiarize the team with what would be going on if actual patients were coming through, and team members needed to know where all the supplies were in the decontamination response van and also

needed to set up the shower tent and make all the water connections to the tent. While there are no federal or state requirements as to how often decontamination drills need to be held, Kimble said, the hospital is required to conduct disaster drills at least twice a year.
Source: http://www.eldoradotimes.com/articles/2005/06/20/news/news2. txt

[Return to top]

Information Technology and Telecommunications Sector

25. *June 21, Associated Press* — **Blackberry network down for hours.** The BlackBerry e−mail service suffered a nationwide outage Friday morning, June 17, but the nearly four−hour disruption only appeared to affect devices connected to certain types of cellular networks. Although Research in Motion Ltd. (RIM), which makes the popular mobile devices and provides a service connecting them to corporate networks, did not respond to phone calls seeking comment, Cingular Wireless, T−Mobile USA, and Nextel Communications Incorporated confirmed the outage. Cingular Wireless said RIM's outage lasted for three hours and 49 minutes, while T−Mobile USA said service was restored by noon EDT. Nextel Communication Incorporated reported that only some customers experienced trouble, and in those cases it was a delay in e−mails rather than a full−fledged service disruption. Both Verizon Wireless and Sprint Corporation said there were no complaints from their customers at all, possibly due to their reliance on cellular networks based on a technology called Code Division Multiple Access (CDMA); the three cellular carriers who experienced the service disruption rely on alternate technology−based cellular networks other than CDMA.
Source: http://www.nytimes.com/aponline/technology/AP−Blackberry−Out age.html?

26. *June 20, SecurityTracker* — **Cisco VPN 3000 lets remote users determine valid groupnames.** A vulnerability was reported in the Cisco VPN 3000 concentrators. A remote user can determine valid groupnames. When groupname authentication is used, the system provides a different response to a connection request with a valid groupname than it does with an invalid groupname. A remote user can connect to the target system repeatedly and send an IKE Aggressive Mode packet using different groupnames to attempt to determine valid groupnames. The system will respond only to packets with a valid groupname. The vendor has released a fixed version (4.1.7.F).
Source: http://securitytracker.com/alerts/2005/Jun/1014246.html

27. *June 20, CNET News* — **Security tools face increased attack according to research group.** As the pool of easily exploitable Windows security bugs dries up, hackers are looking for holes in security software to break into PCs, Yankee Group analysts said in a research paper published Monday, June 20. According to the Yankee Group, software makers of ubiquitous antivirus products have not yet been forced to acknowledge and fix potential problems in their code. Microsoft's Windows operating system has been a favorite target of hackers, but new security flaws are being discovered in security products at a faster rate than in Microsoft's products, the analysts wrote. Symantec, F−Secure and CheckPoint Software Technologies are among the vendors that have seen a rise in the number of security issues that affect their products in the past years and the Yankee Group predicts a "rising tide" of vulnerabilities will soon be found in security products.
Yankee Group findings: http://www.yankeegroup.com/public/news_releases/news_release

_detail.jsp?ID=PressReleases/news_06202005_FearandLoathing_P R.htm
Source: http://news.com.com/Security+tools+face+increased+attack/2100−1002_3−5754773.html?tag=nefd.top

Internet Alert Dashboard

DHS/US−CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

US−CERT Operations Center Synopsis: Activity on one of the ports associated with Windows' Server Message Block (SMB) protocol is climbing. A surge in activity targeting TCP port 445, which is associated with SMB related communications on Windows machines has been observed. This may indicate an increase in known attacks, such as password brute forcing, or the exploitation of known vulnerabilities, or may indicate activity related to the recent Microsoft Incoming SMB Packet Validation Remote Buffer Overflow Vulnerability.

Current Port Attacks

Top 10 Target Ports	445 (microsoft−ds), 135 (epmap), 1026 (−−−), 6881 (bittorrent), 27015 (halflife), 139 (netbios−ssn), 53 (domain), 137 (netbios−ns), 18152 (−−−), 80 (www) Source: http://isc.incidents.org/top10.html; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

Nothing to report.
[Return to top]

General Sector

Nothing to report.
[Return to top]

DHS/IAIP Products & Contact Information

The Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) serves as a national critical infrastructure threat assessment, warning, vulnerability entity. The IAIP provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures:

DHS/IAIP Daily Open Source Infrastructure Reports − The DHS/IAIP Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS/IAIP Daily Open Source Infrastructure Report is available on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

Homeland Security Advisories and Information Bulletins − DHS/IAIP produces two levels of infrastructure warnings. Collectively, these threat warning products will be based on material that is significant, credible, timely, and that addresses cyber and/or infrastructure dimensions with possibly significant impact. Homeland Security Advisories and Information Bulletins are available on the Department of Homeland Security Website: http://www.dhs.gov/dhspublic/display?theme=70

DHS/IAIP Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS/IAIP Daily Report Team at (703) 983−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS/IAIP Daily Report Team at (703) 983−3644 for more information.

Contact DHS/IAIP

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

DHS/IAIP Disclaimer

The DHS/IAIP Daily Open Source Infrastructure Report is a non−commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.